WIRELESS NETWORK HAVING MULTIPLE COMMUNICATION ALLOWANCES

This application claims priority to U.S.Provisional Serial No. 60/454,694 filed March 14, 2003.

FIELD OF INVENTION

Wireless networks are well-known, and may be based, for example, on the 802.11 standard. Because the contents of the wireless network can be received by anyone with wireless access, security may be achieved through encryption of the stream. Anyone with an encryption code can tap into the network. Those without the encryption code, however, simply cannot decode the wireless stream. In addition, standard network protocols may be used, so that not only the encryption code, but also a network login, is necessary.

SUMMARY

The present application describes a wireless network, defining a plurality of different classes of service, where the different classes of service include at least a first class of service that includes a first set of

permissions for access to resources, and a second class of service which includes a second set of permissions of access to resources.

BRIEF DESCRIPTION OF THE DRAWINGS

Thes and other aspects will now be described in detail with reference to the accompanying drawings, in which:

Figure 1 shows a basic diagram of the networks described herein.

DETAILED DESCRIPTION

Wireless networks have been used for other things besides secure file transfer. For example, Internet Cafes, and "wireless hot spots" may include the capability of communication to a user's personal laptop which is equipped with a wireless card. This may use a network key for the encryption of the word "public", or a network key which is given to users who pay for the service or pay for a drink or food, or without any network key at all. Certain areas such as hotel rooms are often wireless enabled. However, the communication is typically or totally on, or totally off; that is either the user is allowed to receive wireless Internet, or the user is blocked from all communications.

The present system teaches a network with multiple levels of capability, depending on the access credentials possessed by the user. Figure 1 shows this being carried out using multiple network cards or NICs. However, the same effect can be obtained with a single NIC. Preferably the network cards are wireless, using one of the features of IEEE 802.11 wireless communication protocols.

Different classes of users may be assigned. The first class of users, shown as user 1, are allowed file access to files and information from the server. These users may be given the encryption key, here for the first NIC 100 here shown as ABCDEF. These users may be allowed the highest level of access to resouces. As conventional users who have the complete set of credentials, they are allowed unlimited upload and download, and full file access (that is allowed to non-administrator users). In addition, these users may be allowed the maximum upload and download speeds which is given to network users, and to receive all different kinds of Internet and files from all sources.

For example, the amount of access which is provided to these users may be assigned by the operating system which drives the NICS. For example, if Windows XP is used as the operating system, it

may assign NIC 100 with unlimited file access.

A second class of users shown as user 2 do not have the credentials, here the encryption key, for the network card 100, and hence use the encryption key "public" and thereby can only communicate with the network card No. 2 shown as 110. Alternatively, these same users may communicate using no encryption key at all. The network card 110 allows only some subset of the operations that are allowed by the network card 100. For example, the user 2 may receive Internet only, and no file access. They may be allowed to print. In addition, the upload and download speeds may be limited or severely limited ; for example, the Internet may be limited to 1M download speeds and 100K of upload speed.

This system as described above may be usable in an office environment. For example, users who are actually members of the office obtain file access, while visitors only receive print and Internet access.

Another contemplated use is in pay-for-Internet use. The user 1 may pay a higher fee than the user 2. For example, user 2 may pay only for limited Internet, while user 1 may pay for access to resources such as video over IP, and higher download speeds from the Internet.

In addition, a third class of users shown as user 3 may be defined. These users communicate only to NIC 120. Note that while this describes users 1, 2 and 3, any subset of these users may be used, for example a system may be configured which only communicates with user 1 and user 3. The NIC No. 3 is shown as having no encryption code whatsoever. User 3 is limited even further. User 3 may receive only commercial parts of the Internet. In the office environment, this may limit the Internet to web pages describing the office and/or certain intranet sites. In a pay for internet environment, this may describe the "free" user, who may only receive certain content. User 3 may also receive a severely restricted bandwidth and/or only a limited quantity of information. For example, the user 3 may be assigned a token which allows them only to receive for example total of 1 megabytes of download and only to upload 100 Kilobytes of upload. This even further limits the user 3.

As described above, the different users in their different classes have different levels of file access, and resource access, resource speed and resource amount.

Figure 1 shows this being carried out with three different network cards over the same airspace. Alternatively, the three different

networks may be carried out as part of a single network card; shown as network card 130. For example, this may include three network resources which operate on the single card. Alternatively, the three different kinds of resources may be carried out in software, for example this may be carried out by three different network resource allowances within the software that runs the network card or within the server 99.

Other implementations are within the disclosed embodiment